

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-202659

(43)Date of publication of application : 09.08.1996

(51)Int.Cl.

G06F 15/00  
G06F 12/00  
H04L 12/28  
H04M 1/66  
// H04M 3/42

(21)Application number : 07-012187

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 30.01.1995

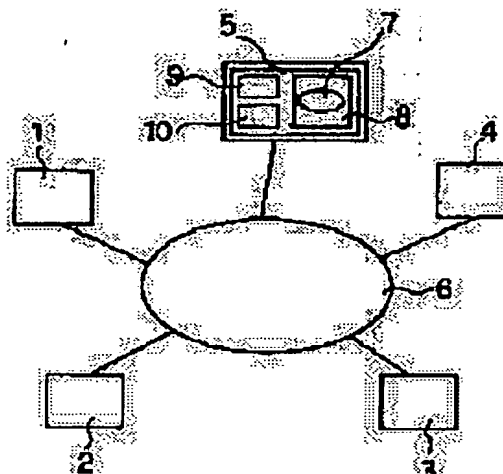
(72)Inventor : FUKUMOTO YUJI  
NAKACHI TOSHIYUKI

## (54) COMMON INFORMATION PROCESSING SYSTEM

### (57)Abstract:

**PURPOSE:** To protect common information against alteration individually by managing the information showing whether a terminal is permitted to access the common information and permitting only a terminal which is permitted to access the common information according to the managed information.

**CONSTITUTION:** To offer the common information 7 to a conference server 5 from a terminal 1 as owner, a document number, owner information (terminal 1 in this case), and connection information (terminals 2 and 4 in this case), are added to a document when the common information 7 is the document. The conference server 5 receives a request to access the common information 7, judges whether or not the terminal is the owner of the common information on the basis of the owner information, and allows access when so. When the terminal is not the owner, on the other hand, it is judged from the connection information whether or not a connection with the owner is set, and access is allowed when the connection is set, but rejected when not.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-202659

(43) 公開日 平成8年(1996)8月9日

(51) Int. Cl. <sup>6</sup>

識別記号

F I

G06F 15/00

330 B 9364-5L

12/00

572 A

H04L 12/28

H04M 1/66

C

H04L 11/00

310

D

審査請求 未請求 請求項の数 4 O L (全8頁) 最終頁に続く

(21) 出願番号

特願平7-12187

(22) 出願日

平成7年(1995)1月30日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 福元 勇二

東京都日野市旭が丘3丁目1番地の1 株  
式会社東芝日野工場内

(72) 発明者 仲治 俊行

東京都日野市旭が丘3丁目1番地の1 株  
式会社東芝日野工場内

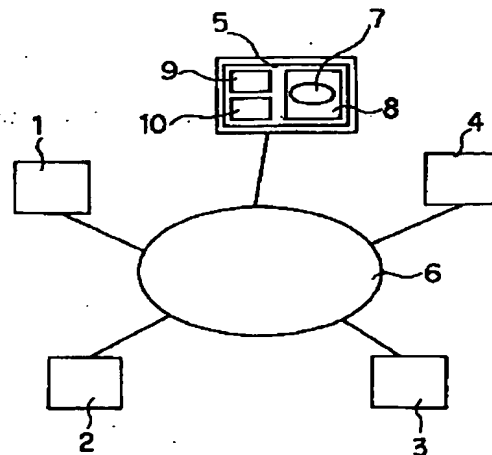
(74) 代理人 弁理士 須山 佐一

(54) 【発明の名称】 共有情報処理システム

(57) 【要約】

【目的】 共有情報個別に改変保護を行うことのできる共有情報処理システムの提供。

【構成】 端末1～4より共有情報7へのアクセスがあったときに当該端末1～4に対してアクセスを許可するかどうかの情報を管理し、この管理情報に基づき、アクセスが許可された端末1～4にのみ共有情報7へのアクセスを許可する。



**【特許請求の範囲】**

**【請求項 1】** 複数の端末がネットワークを介して接続され、各端末がこれら端末間の共有情報をアクセスして書き替え可能とされた共有情報処理システムにおいて、前記端末より前記共有情報へのアクセスがあったときに当該端末に対してアクセスを許可するかどうかの情報を管理する手段と、

この管理情報に基づき、アクセスが許可された端末にのみ前記共有情報へのアクセスを許可する手段とを具備することを特徴とする共有情報処理システム。

**【請求項 2】** 複数の端末がネットワークを介して接続され、各端末がこれら端末間の共有情報をアクセスして書き替え可能とされた共有情報処理システムにおいて、前記端末より前記共有情報へのアクセスがあったとき、当該端末が当該共有情報のオーナーかどうかを判別する手段と、

当該端末が当該共有情報のオーナーでないとき、当該端末がオーナーとの間でコネクションがあるかどうかを判別する手段と、

当該端末がオーナーとの間でコネクションがあるとき、当該端末より入力された ID コードまたはパスワードの正誤を判別する手段と、

当該端末が当該共有情報のオーナーまたは当該端末より正しい ID コードもしくはパスワードが入力されたときのみ前記共有情報へのアクセスを許可する手段とを具備することを特徴とする共有情報処理システム。

**【請求項 3】** 共有情報へのアクセスの許可をするかどうかの管理を、書き込みと読み込みとを別々に行うことを特徴とする請求項 1 または 2 記載の共有情報処理システム。

**【請求項 4】** 書き替えられた共有情報を書き替え前の共有情報とは別に管理することを特徴とする請求項 1 乃至 3 のいずれかに記載の共有情報処理システム。

**【発明の詳細な説明】****【0001】**

**【産業上の利用分野】** 本発明は、例えばネットワークを介してコンピュータを利用して共同作業を行う場合に共有情報に対する改変を保護する共有情報処理システムに関する。

**【0002】**

**【従来の技術】** 従来、共有ウィンドウでの作業または共同作業をネットワークを介して行うときは、共有情報が蓄積されている装置へログイン等を行って情報の書き込みを行っていた。また、共有情報を蓄積しておくディスクやディレクトリを指定しておき、そのディスクやディレクトリに対する書き込み、読み込み権をグループ員にのみ許可する事によって共有情報の改変保護を行ってきた。このような従来の方法ではディスクやディレクトリ単位でしか改変に対する保護を行えず、共有情報個別の改変に対する保護を行えないという問題があった。そこ

で、共有情報の 1 つ 1 つについて別々にディスクやディレクトリを準備することで改変に対する保護を行うことが考えられるが、この場合非効率であるという問題が生じる。

**【0003】**

**【発明が解決しようとする課題】** 上述の如く、従来の方法では共有情報に対してディスクやディレクトリ単位の改変保護となっており、共有情報個別に改変保護を行えないという問題点があった。

10 **【0004】** そこで、本発明は、このような問題点を除去し、共有情報個別に改変保護を行うことのできる共有情報処理システムを提供することを目的としている。

**【0005】**

**【課題を解決するための手段】** 本発明は、かかる課題を解決するため、複数の端末がネットワークを介して接続され、各端末がこれら端末間の共有情報をアクセスして書き替え可能とされた共有情報処理システムにおいて、前記端末より前記共有情報へのアクセスがあったときに当該端末に対してアクセスを許可するかどうかの情報を管理する手段と、この管理情報に基づき、アクセスが許可された端末にのみ前記共有情報へのアクセスを許可する手段とを具備する。

20 **【0006】** 別の態様の発明は、複数の端末がネットワークを介して接続され、各端末がこれら端末間の共有情報をアクセスして書き替え可能とされた共有情報処理システムにおいて、前記端末より前記共有情報へのアクセスがあったとき、当該端末が当該共有情報のオーナーかどうかを判別する手段と、当該端末が当該共有情報のオーナーでないとき、当該端末がオーナーとの間でコネクションがあるかどうかを判別する手段と、当該端末がオーナーとの間でコネクションがあるとき、当該端末より入力された ID コードまたはパスワードの正誤を判別する手段と、当該端末が当該共有情報のオーナーまたは当該端末より正しい ID コードもしくはパスワードが入力されたときのみ前記共有情報へのアクセスを許可する手段とを具備する。

30 **【0007】** 上記発明において、共有情報へのアクセスの許可をするかどうかの管理を、書き込みと読み込みとを別々に行うようにしてもよいし、書き替えられた共有情報を書き替え前の共有情報とは別に管理するようにしてもよい。

**【0008】**

**【作用】** 本発明では、端末より前記共有情報へのアクセスがあったときに当該端末に対してアクセスを許可するかどうかの情報を管理しておき、この管理情報に基づき、アクセスが許可された端末にのみ共有情報へのアクセスを許可するように構成したので、個別の共有情報に対する無秩序な改変を防ぐことができる。

**【0009】**

50 **【実施例】** 以下、本発明の実施例を図面に基づき説明す

る。

【0010】図1は本発明の一実施例に係るシステムの構成を示す図である。同図において、1～4は端末、5は会議サーバ、6はネットワークを示している。会議サーバ5は、共有情報7を蓄積する情報蓄積部8、アクセス管理部9及びファイリング処理部10を備える。

【0011】このようなシステムにおいて、共同作業を行う場合の動作を説明する。接続が設定されている範囲を図2に示す。同図において、11が接続を設定してある範囲である。ここでは、端末1、2、4及び会議サーバ5間でネットワーク6を介して接続を設定し、会議等の共同作業を行うものとする。すなわち、端末3については接続が設定されていない。

【0012】各端末1～4上には、会議を行う各端末共同に使用する共有情報を表示する共有ウィンドウがあり、この共有ウィンドウ上の情報に対して読み書きする事によって会議を進める。

【0013】図3に各端末1～4のディスプレイの様子を示す。12は端末1のディスプレイ、13は端末2のディスプレイ、14は端末3のディスプレイ、15は端末4のディスプレイを示し、16～19はそれぞれの端末1～4の共有ウィンドウを示す。ここでは端末1、2、4間で共同作業を行うので、図3の共有ウィンドウ16、17、19は同じ資料（共有情報）、例えば“a b c d e f g h i j”を表示している。端末3のディスプレイ上の共有ウィンドウ18は端末1、2、4の共有ウィンドウと同じものは表示できない。端末3のディスプレイ上の共有ウィンドウ18は、例えば“あいうえお かきくけこ”を表示している。

【0014】本実施例では、例えば端末1から会議を行うための共有情報（資料）を提供している場合、端末1が共有情報7のオーナーとなり、その共有情報7のオーナーまたはオーナーへ接続の設定を行っている端末だけ（ここでは、端末1、2、4）が共有情報へアクセス（書き込み、読み込み等）する事ができる。すなわち、端末1に対して接続が設定されていない端末3は、上記共有情報7にアクセスする事ができない。

【0015】オーナーである端末1から会議サーバ5への共有情報の提供は、図4に示すように、共有情報が例えば文書であるときは、文書41に、文書ナンバー42、オーナー情報43（ここでは、端末1）及び接続端末情報44（ここでは、端末2、4）を付して行われる。

【0016】このとき各端末1、2、4は、会議サーバ5へ共有情報7のアクセス要求を行い、共有情報7への書き込み、読み込みを行うものとする、会議サーバ5でのアクセス要求制御フローは図5のようになる。つまり、共有情報7へのアクセス要求を会議サーバ5で受け取り（ステップ501）、その端末が共有情報のオーナー

かどうかの判定を図4のオーナー情報43に基づき行い（ステップ502）、オーナーであればアクセスを許可し（ステップ503）、オーナーでない場合はオーナーとの接続が設定されているかどうかの判断を図4の接続端末情報44に基づき行い（ステップ504）、設定されている場合はアクセスを許可し（ステップ503）、設定されていない場合はアクセスを拒否する（ステップ505）。

【0017】例えば端末1（共有情報のオーナー）から共有情報7へのアクセス要求があった場合、オーナーであるということを経由して会議サーバ5で判断し、共有情報7へのアクセスを許可する。また、端末2からアクセス要求があった場合は、オーナーでないがオーナーと接続が設定されているということでアクセスが許可される。一方、端末3からアクセス要求があった場合、オーナーではない及びオーナーと接続の設定がなされていないことより共有情報へのアクセスが拒否される。この様子を図6に示す。20は共有情報へ許可されたアクセス、21は拒否されたアクセスである。

【0018】また、共有情報提供者（オーナー）または会議サーバ5において共有情報7へのアクセス制限機能を設けることによって、アクセスを行える端末を選択する事が可能となる。その判定のフローを図7に示す。これはアクセス要求が発生した場合（ステップ701）、アクセス要求元がオーナーであるかを判定し（ステップ702）、オーナーであればアクセスを許可し（ステップ703）、オーナーでない場合はオーナーとの接続が設定されているかの判定を行い（ステップ704）、設定されていないときはアクセスを拒否し（ステップ705）、設定されているときはアクセス（書き込み、読み込み）制限がされているかの判定を行い（ステップ706）、制限されている場合はアクセスを拒否し（ステップ705）、制限されていない場合はアクセスを許可する（ステップ703）。

【0019】ここで、端末1、2、4及び会議サーバ5間に接続が設定されており、端末4はアクセス制限を受けている場合についての例を以下に示す。つまり、端末1から提供された共有情報がある場合について考えると、図8に示すように、端末1からアクセス要求があった場合、オーナーであるということでアクセスを許可される。また、端末2からアクセス要求があった場合、オーナーでないが接続が設定され、かつ、アクセス制限がないということでアクセスを許可される。一方、端末3からアクセス要求があった場合、オーナーでなく、かつ、オーナーと接続が設定されていないということでアクセスを拒否される。また、端末4からアクセス要求があった場合、オーナーでないがオーナーと接続が設定されているがアクセス制限があるということでアクセスを拒否される。さらに、アクセス要求を出す端末1～4へのアクセス制限に、IDコー

10

20

30

40

50

ド、パスワード等を利用することができる。つまり、共有情報 7 に ID コードとパスワードを設定しておき、アクセスを許される端末 1 ~ 4 にのみその ID コード、パスワードを知らせておくようにする。この場合、共有情報提供者（オーナー）または会議サーバ 5 がアクセス権の管理を行う。このときの会議サーバ 5 内でのアクセス制御の流れを図 9 に示す。ある端末からアクセス要求があった場合（ステップ 901）、アクセス要求元がオーナーであるかを判断し（ステップ 902）、オーナーであればアクセスを許可し（ステップ 903）、オーナーでない場合はオーナーとのコネクションが設定してあるかの判断を行い（ステップ 904）、設定されていないときはアクセスを拒否し（ステップ 905）、設定してある場合は ID コードとパスワードを要求して正誤を判断し（ステップ 906）、それが正しいときはアクセスを許可し（ステップ 903）、誤っているときはアクセスを拒否する（ステップ 905）。

【0020】例えば、端末 1 が提供した共有情報 7 に対して ID コード“ABCDEFGH”とパスワード“1234”を設定しておく。端末 4 へはこの ID コードとパスワードが知らせてあり、端末 2 には知らせていないとする。

【0021】その場合、図 10 に示すように、端末 1 が共有情報 7 に対してアクセス要求を行った場合、オーナーであることよりアクセスが許可される。一方、端末 2 がアクセス要求を出した場合、オーナーではないがオーナーとのコネクションが設定されているが ID コード及びパスワードが知らされていないことよりアクセスを拒否される。また、端末 3 がアクセス要求を出した場合、オーナーではなく、かつ、オーナーとのコネクションが設定されていないことよりアクセス拒否される。これに対して、端末 4 がアクセス要求を出した場合、オーナーでないがオーナーとコネクションが設定され、かつ、ID コード及びパスワードが知らせてあることよりアクセスが許可される。

【0022】共有情報へのアクセスについて書き込みアクセスと読み込みアクセスを別々に制御する事により、オーナー以外の端末ウィンドウには、共有情報の表示はできるが、書き込みはできない設定を行うことが可能である。このときの制御の流れを図 11 に示す。

【0023】ある端末からアクセス要求があった場合（ステップ 1101）、オーナーかどうかを判断し（ステップ 1102）、オーナーのときは書き込みアクセスと読み込みアクセスを許可する（ステップ 1103、1104）。一方、オーナーでないときは、オーナーとコネクションの設定がなされているかの判断を行い（ステップ 1105）、設定されていないときは書き込みアクセスと読み込みアクセスを拒否する（ステップ 1106）。設定されているときは、書き込み要求か読み込み要求かの判断を行う（ステップ 1107）。そして、書き込み要求

のときは、書き込み制限があるかの判断を行い（ステップ 1108）、制限があるときは書き込みアクセスと読み込みアクセスが拒否され（ステップ 1106）、制限がないときは書き込みアクセスのみが許可される（ステップ 1103）。一方、読み込み要求のときは、読み込み制限があるかの判断を行い（ステップ 1109）、制限があるときは書き込みアクセスと読み込みアクセスが拒否され（ステップ 1106）、制限がないときは読み込みアクセスのみが許可される（ステップ 1104）。

10 書き込みが禁止されている共有情報に対して書き込みを行いたい場合が考えられる。このような場合は共有情報ファイルの書換は行わずに共有情報に関連した形で各端末 1 ~ 4 が別ファイルをもって蓄積することができる。図 12 にこのときの例を示す。図 12 において、21 は共有情報（共有情報ファイルに会議サーバ内で蓄積）、22 は書き込み用情報（共有情報とは別のファイルで各端末内で蓄積）、23 は共有情報と書き込み用情報を合成したものである。共有情報内には資料として“ABCDE アイウエオ”が書いてあり、書き込み用情報で共有情報の文章へアンダーラインを引いている。元々の共有情報ファイルを改変することなく共有情報へ書き込みを行える。

【0024】なお、共有情報を端末 1 から提供する場合、図 4 に示した情報ばかりでなく、共有情報に転送日時及びシリアル番号、著作権マーク等を書き込むことによりオーナーとそれを区別できる。また、書き込み等を許可される端末から書き込みがあった場合は自動的に書換日時や書換者及び著作権マーク等を書き込む機能を備えることにより、いつ誰が書換を行ったかをいつでも確認する事ができる。

【0025】また、以上の実施例で述べた機能は会議サーバのみで実現されるのではなく、同様の機能を共有情報提供者側で持つことも考えられる。この場合、共有情報を提供できる全ての端末へ上記の機能の一部または全部を備えることが必要となるが、専用の会議サーバは不要となる。

【0026】

【発明の効果】以上説明したように、本発明によれば、共有情報に対してそのオーナー以外にコネクションの設定、書き込み及び読み込み制限、ID コード及びパスワードの設定、読み込みアクセスと書き込みアクセスの別々の制御、及び書き込み用ファイルを別に蓄積する等の制御を行うことにより、共有情報の改変に対する保護を行えるという利点がある。共有ウィンドウに共有情報を表示及び書き込み等を行うことによって会議等の共同作業を実現する場合に、提供した共有情報がむやみに書換えられたり、会議をはじめるときに以前の共有情報と比較して無断で変更等を加えられていたりするといった事態を避けることが可能である。

50 【図面の簡単な説明】

【図 1】本発明の一実施例に係るシステムの構成を示す図である。

【図 2】本発明の一実施例に係る接続設定範囲を示す図である。

【図 3】本発明の一実施例に係る端末のディスプレイ上の共有ウィンドウを示す図である。

【図 4】本発明の一実施例に係る共有情報の内容を示す図である。

【図 5】本発明の一実施例に係る共有情報に対するアクセスでオーナーとの接続の有無での判定の流れ図である。

【図 6】図 5 の流れ図に従ったときの各端末からのアクセスを示す図である。

【図 7】本発明の一実施例に係るアクセス制限を設けたときのアクセスの判定を行う流れ図である。

【図 8】図 7 の流れ図に従ったときの各端末からのアクセスを示す図。

【図 9】本発明の一実施例に係る共有情報に ID コード及びパスワードを付けたときのアクセス判定制御の流れ

図である。

【図 1 0】図 9 の流れに従ったときの各端末からのアクセスを示す図。

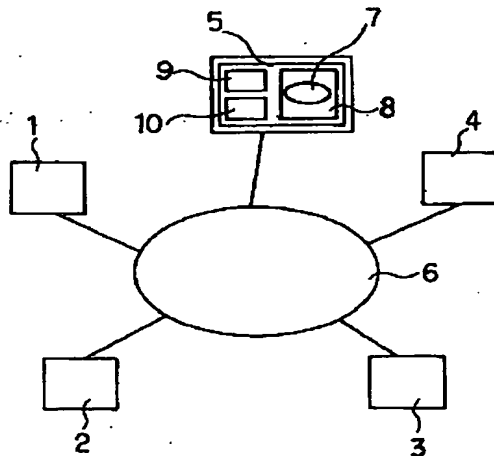
【図 1 1】本発明の一実施例に係る書き込みと読み込みと別々にアクセスの制御を行うときの流れ図である。

【図 1 2】本発明の一実施例に係る書き込み禁止の共有情報に書き込みを行うとき別ファイルを使うときの説明図である。

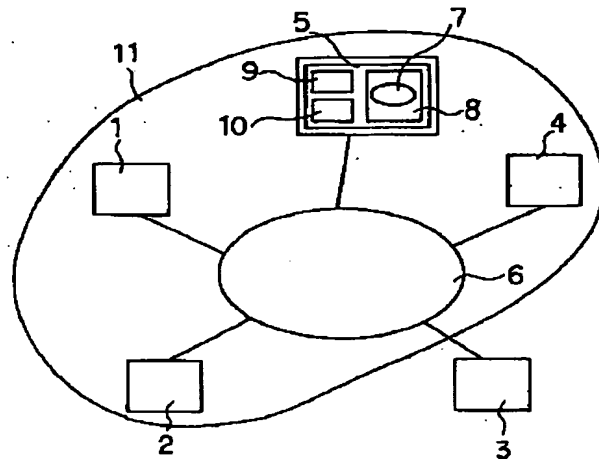
#### 【符号の説明】

- 1 ～ 4 ……端末
- 5 ……会議サーバ
- 6 ……ネットワーク
- 7 ……共有情報（端末 1 提供）
- 8 ……情報蓄積部
- 9 ……アクセス権管理部
- 1 0 ……ファイリング処理部
- 1 1 ……接続設定範囲
- 1 2 ～ 1 5 ……端末のディスプレイ
- 1 6 ～ 1 9 ……共有ウィンドウ

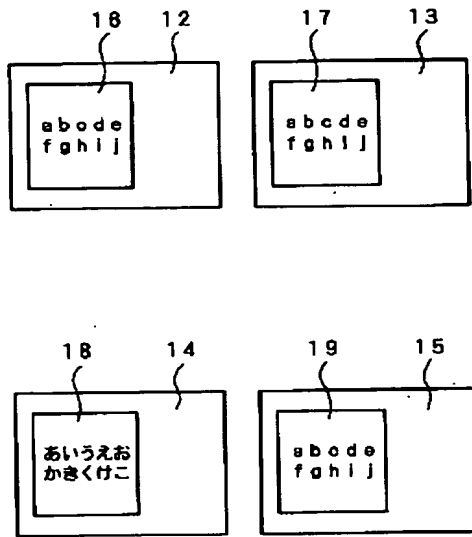
【図 1】



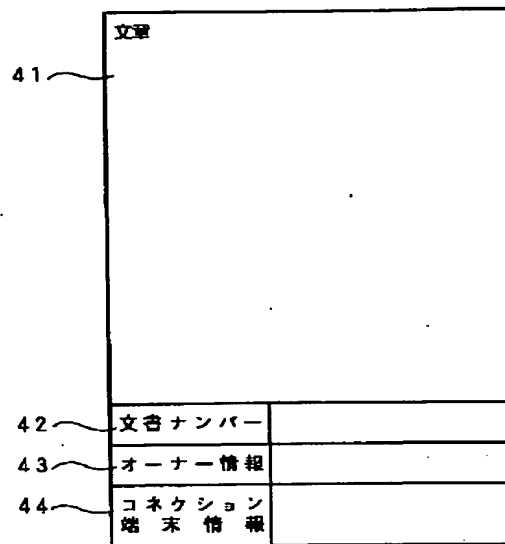
【図 2】



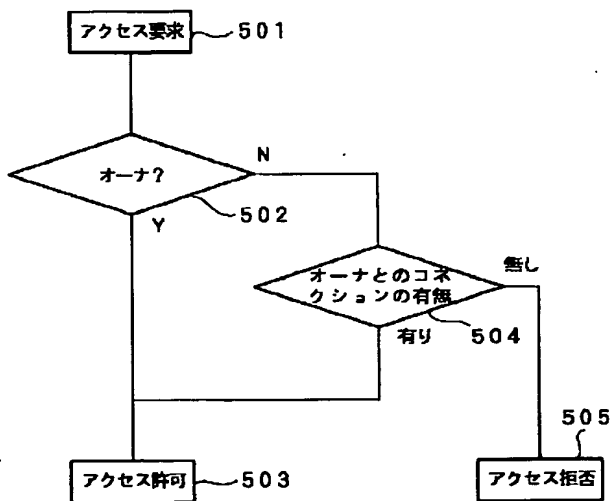
【図3】



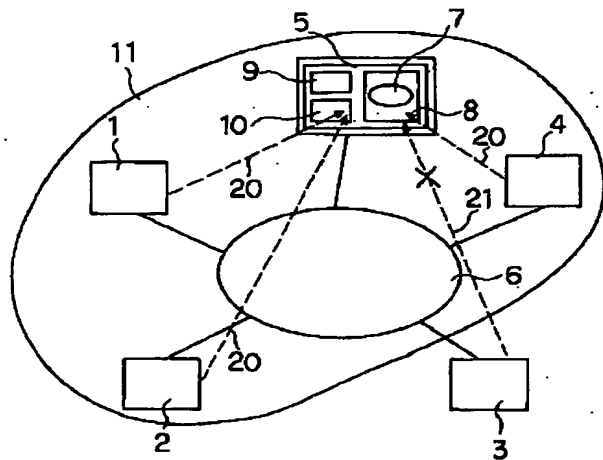
【図4】



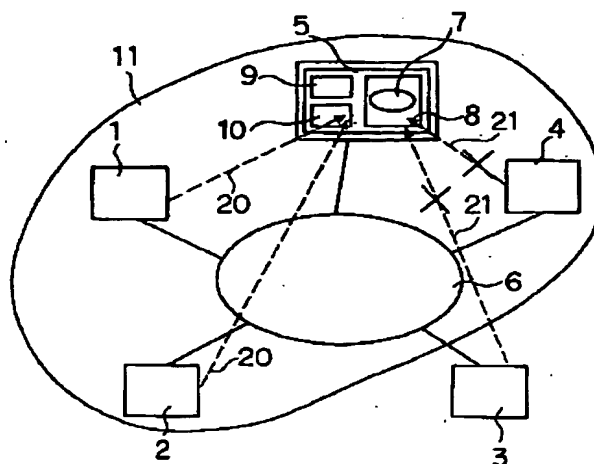
【図5】



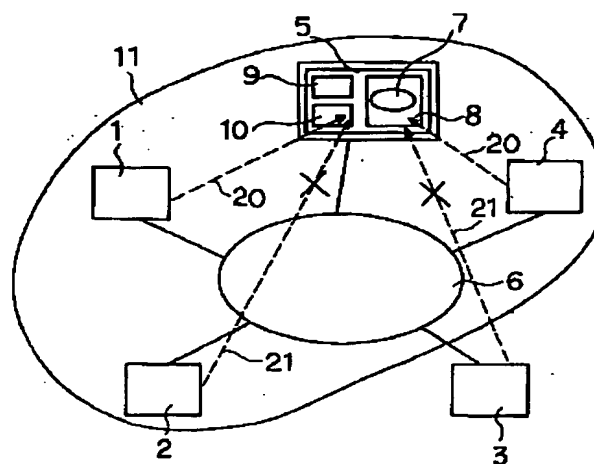
【図6】



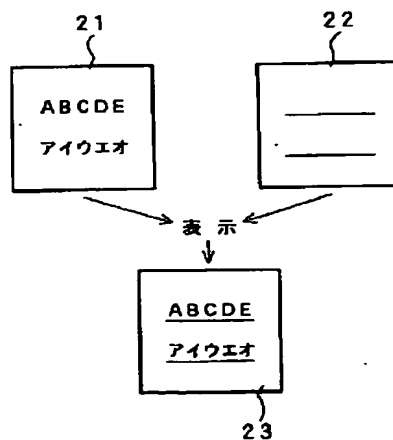
【图8】



【図 10】

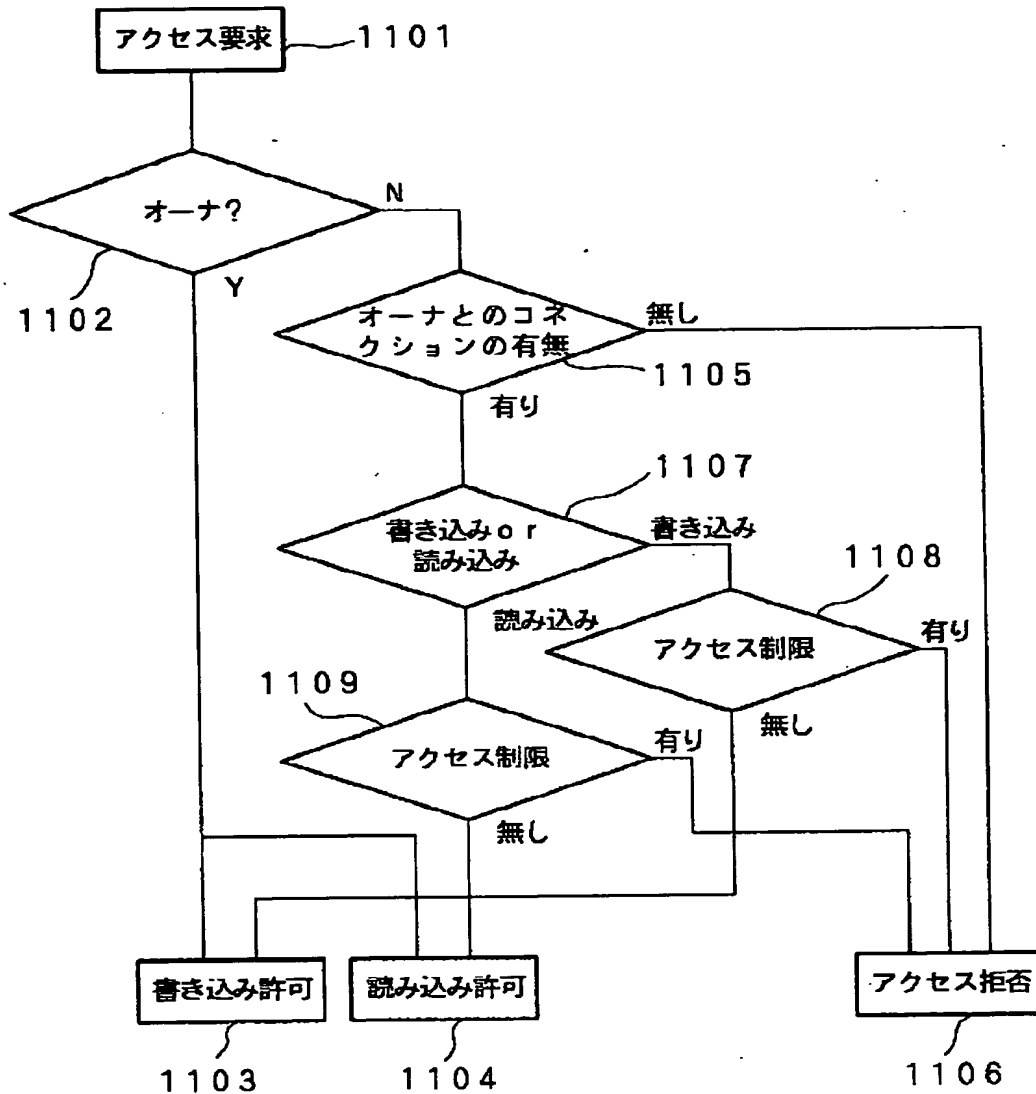


【图 1 2】





【図 1 1】



フロントページの続き

(51) Int. Cl.<sup>6</sup>

識別記号

弁内整理番号

F I

技術表示箇所

// H 0 4 M 3/42

Z